

AMENDMENT TO THE CLAIMS

1-16. (Cancelled)

17. (Currently Amended) A method of redirecting data items from a messaging host system to a user's mobile device, comprising the steps of:

detecting a new data item for the user at the messaging host system;

forwarding a copy of the new data item to a redirector host system;

determining whether the new data item should be redirected from the redirector host system to the user's mobile device; ~~and~~

if the new data item should be redirected, then using the redirector host system to automatically encrypt ~~encrypting~~ the new data item to form an encrypted new data item using a cipher algorithm and an encryption key to encrypt the new data item; ~~and~~

packaging the encrypted new data item into an electronic envelope and transmitting the electronic envelope to the user's mobile device;

receiving the electronic envelope at the user's mobile device;

extracting the encrypted new data item from the electronic envelope; ~~and~~

decrypting the encrypted new data item using a cipher algorithm and a decryption key to decrypt the encrypted new data item to recover the new data item;

generating the encryption key at a computer system associated with the mobile device;

forwarding the encryption key from the computer system to the redirector host system using a secure communications link;

generating the decryption key at the computer system associated with the mobile device; and

forwarding the decryption key from the computer system to the mobile device using a secure communications link.

18. (Original) The method of claim 17, wherein the step of forwarding the decryption key comprises:

sending the decryption key to the mobile device over a serial connection between the computer system and the mobile device.

19. (Currently Amended) A method of redirecting data items from a messaging host system to a user's mobile device, comprising the steps of:

detecting a new data item for the user at the messaging host system;

forwarding a copy of the new data item to a redirector host system;

determining whether the new data item should be redirected from the redirector host system to the user's mobile device; ~~and~~

if the new data item should be redirected, then using the redirector host system to automatically encrypt ~~encrypting~~ the new data item to form an encrypted new data item using a cipher algorithm and an encryption key to encrypt the new data item; ~~and~~

packaging the encrypted new data item into an electronic envelope and transmitting the electronic envelope to the user's mobile device;

receiving the electronic envelope at the user's mobile device;

extracting the encrypted new data item from the electronic envelope; ~~and~~

decrypting the encrypted new data item to recover the new data item.

using a cipher algorithm and a decryption key to decrypt the encrypted new data item.

using a cipher algorithm and an encryption key to encrypt the new data item;

generating a private key to be used as the decryption key at a computer system associated with the mobile device;

forwarding the private key from the redirector host system to the mobile device using a secure communications link;

generating a public key to be used as the encryption key at the computer system; and

forwarding the public key from the computer system to a public key repository.

20. (Original) The method of claim 19, further comprising the step of: forwarding the public key from the computer system to the redirector host system.

21-104. (Cancelled)

105. (Previously Presented) The method of claim 17, further comprising:

storing the new data item in a user's inbox coupled to the messaging host system.

106. (Previously Presented) The method of claim 17, wherein the detecting step includes the steps of:

determining whether a new data item has been received at the messaging host system for a particular user; and

checking a forwarding file coupled to the messaging host system to determine whether the particular user's data items should be redirected to the redirector host system.

107. (Previously Presented) The method of claim 106, wherein the forwarding file includes a list of system addresses where the user's data items should be forwarded by the messaging host system.

108. (Previously Presented) The method of claim 17, further comprising the steps of:

configuring a set of filtering rules for use by the redirector host system in determining whether the new data item should be redirected to the user's mobile device; and

providing an access mechanism that allows the user to remotely configure and reconfigure the set of filtering rules.

109. (Previously Presented) The method of claim 17, further comprising the steps of:

configuring a user profile database for use by the redirector host system in determining whether the new data item should be redirected to the user's mobile data device; and

providing an access mechanism that allows a system administrator of the messaging host system to remotely configure and reconfigure the user profile database.

110. (Previously Presented) The method of claim 17, further comprising the step of:

storing the new data item within a memory of the mobile device.

111. (Previously Presented) The method of claim 17, wherein the decryption key is generated at the redirector host system; and

the decryption key is forwarded from the redirector host system to the mobile device using a secure communication link.

112. (Previously Presented) The method of claim 17, wherein the step of forwarding the decryption key comprises:

forwarding the decryption key to the mobile device using Internet Message Access Protocol (IMAP) over Secure Sockets Layer (SSL) protocol.

113. (Previously Presented) The method of claim 17, further comprising the steps of:

preparing a reply data item at the mobile device that is related to the new data item;

encrypting the reply data item at the mobile device to form an encrypted reply data item; and

packaging the encrypted reply data item into an electronic envelope and transmitting the electronic envelope to the redirector host system.

114. (Previously Presented) The method of claim 113, wherein the electronic envelope packaged with the encrypted reply data item is addressed using an electronic address of the redirector host system.

115. (Previously Presented) The method of claim 114, further comprising the steps of:

extracting the encrypted reply data item from the electronic envelope at the redirector host system;

decrypting the extracted, encrypted reply data item to recover the reply data item;

reconfiguring addressing information associated with the reply data item; and

transmitting the reconfigured reply data item to the messaging host system.

116. (Previously Presented) The method of claim 115, further comprising the steps of:

receiving the reconfigured reply data item at the messaging host system; and

storing the reply data item in a user's inbox coupled to the messaging host system.

117. (Previously Presented) The method of claim 114, further comprising the steps of:

extracting the encrypted reply data item from the electronic envelope at the redirector host system;

decrypting the extracted, encrypted reply data item to recover the reply data item;

reconfiguring addressing information associated with the reply data item; and

transmitting the reconfigured reply data item to a destination system using an electronic address included in the reply data item.

118. (Previously Presented) The method of claim 17, further comprising the steps of:

providing the user's mobile device with an interface to a wireless data network;

forwarding the electronic envelope from the redirector host system to a wireless gateway system;

and

transmitting the electronic envelope from the wireless gateway system to the user's mobile device using the wireless data network.

119. (Previously Presented) The method of claim 17, further comprising the steps of:

transmitting a deactivation message from the user to the redirector host system; and
upon receiving the deactivation message, prohibiting the redirection of data items for the user
sending the deactivation message.

120. (Previously Presented) The method of claim 17, wherein the determining step includes the steps of:
accessing a user profile database including a list of authorized users; and
checking whether the user associated with the new data item is an authorized user to determine
whether the new data item should be redirected to the user's mobile device.

121. (Previously Presented) The method of claim 17, wherein the determining step includes the steps of:
accessing a filter rules database including a list of filters to be applied to data items for a
particular user; and
applying the filters to the new data item to determine whether the new data item should be
redirected to the user's mobile device.

122. (Previously Presented) The method of claim 17, wherein the packaging step includes the step of
addressing the electronic envelope using the electronic address of the user's mobile device.

123. (Previously Presented) The method of claim 17, wherein the data items are E-mail messages, and
wherein the messaging host system is an E-mail host system.

124. (Previously Presented) The method of claim 17, wherein the user's mobile device is a laptop
computer.

125. (Previously Presented) The method of claim 17, wherein the user's mobile device is a two-way
paging computer.

126. (Previously Presented) The method of claim 125, wherein the two-way paging computer includes a wireless network interface for communicating with the redirector host system via a wireless data network.

127. (Previously Presented) The method of claim 126, wherein the redirector host system is coupled to the wireless data network via a wireless gateway system.

128. (Previously Presented) The method of claim 127, wherein the electronic envelope is addressed using the wireless data network address of the two-way paging computer.

129. (Previously Presented) The method of claim 17, wherein the messaging host system is an Internet Service Provider.

130. (Previously Presented) The method of claim 129, wherein the data items are E-mail messages, and wherein the Internet Service Provider includes a mail server program.

131. (Previously Presented) The method of claim 130, wherein the Internet Service Provider further includes a forwarding database coupled to the mail server program for detecting whether a new data item received at the mail server should be forwarded to a redirector host system, and for determining the electronic address of that redirector host system.

132. (Previously Presented) The method of claim 17, wherein the messaging host system and the redirector host system are coupled via the Internet.

133. (Previously Presented) The method of claim 17, wherein the redirector host system includes a further messaging host system.

134. (Previously Presented) The method of claim 17, wherein the redirector host system is incorporated with the messaging host system.

135. (Previously Presented) The method of claim 109, wherein the access mechanism for remotely configuring and reconfiguring the filtering rules is a web-page interface.

136. (Previously Presented) The method of claim 110, wherein the access mechanism for remotely configuring and reconfiguring the user profile database is a web-page interface.

137. (Previously Presented) The method of claim 17, further comprising the steps of:

configuring a user profile database for use by the redirector host system in determining whether the new data item should be redirected to the user's mobile data device; and
storing, within the user profile database, the electronic address of the user's mobile device.

138. (Previously Presented) The method of claim 137, further comprising the step of:

storing, within the user profile database, information regarding the type and configuration of the user's mobile device.

139. (Previously Presented) The method of claim 17, wherein the packaging step further includes the steps of:

converting the encrypted new data item into a compressed format; and
placing the compressed new data item into an electronic envelope that is addressed using the electronic address of the user's mobile device.

140. (Previously Presented) The method of claim 19, storing the new data item in a user's inbox coupled to the messaging host system.

141. (Previously Presented) The method of claim 19, wherein the detecting step includes the steps of:

determining whether a new data item has been received at the messaging host system for a particular user; and

checking a forwarding file coupled to the messaging host system to determine whether the particular user's data items should be redirected to the redirector host system.

142. (Previously Presented) The method of claim 141, wherein the forwarding file includes a list of system addresses where the user's data items should be forwarded by the messaging host system.

143. (Previously Presented) The method of claim 19, further comprising the steps of:

configuring a set of filtering rules for use by the redirector host system in determining whether the new data item should be redirected to the user's mobile device; and

providing an access mechanism that allows the user to remotely configure and reconfigure the set of filtering rules.

144. (Previously Presented) The method of claim 19, further comprising the steps of:

configuring a user profile database for use by the redirector host system in determining whether the new data item should be redirected to the user's mobile data device; and

providing an access mechanism that allows a system administrator of the messaging host system to remotely configure and reconfigure the user profile database.

145. (Previously Presented) The method of claim 19, further comprising the step of:

storing the new data item within a memory of the mobile device.

146. (Previously Presented) The method of claim 19, wherein the decryption key is generated at the redirector host system; and

the decryption key is forwarded from the redirector host system to the mobile device using a secure communication link.

147. (Previously Presented) The method of claim 19, wherein the step of forwarding the decryption key comprises:

forwarding the decryption key to the mobile device using Internet Message Access Protocol (IMAP) over Secure Sockets Layer (SSL) protocol.

148. (Previously Presented) The method of claim 19, further comprising the steps of:

preparing a reply data item at the mobile device that is related to the new data item;
encrypting the reply data item at the mobile device to form an encrypted reply data item; and
packaging the encrypted reply data item into an electronic envelope and transmitting the electronic envelope to the redirector host system.

149. (Previously Presented) The method of claim 148, wherein the electronic envelope packaged with the encrypted reply data item is addressed using an electronic address of the redirector host system.

150. (Previously Presented) The method of claim 149, further comprising the steps of:

extracting the encrypted reply data item from the electronic envelope at the redirector host system;

decrypting the extracted, encrypted reply data item to recover the reply data item;

reconfiguring addressing information associated with the reply data item; and

transmitting the reconfigured reply data item to the messaging host system.

151. (Previously Presented) The method of claim 150, further comprising the steps of:

receiving the reconfigured reply data item at the messaging host system; and
storing the reply data item in a user's inbox coupled to the messaging host system.

152. (Previously Presented) The method of claim 149, further comprising the steps of:

extracting the encrypted reply data item from the electronic envelope at the redirector host system;
decrypting the extracted, encrypted reply data item to recover the reply data item;
reconfiguring addressing information associated with the reply data item; and
transmitting the reconfigured reply data item to a destination system using an electronic address included in the reply data item.

153. (Previously Presented) The method of claim 19, further comprising the steps of:

providing the user's mobile device with an interface to a wireless data network;
forwarding the electronic envelope from the redirector host system to a wireless gateway system;
and
transmitting the electronic envelope from the wireless gateway system to the user's mobile device using the wireless data network.

154. (Previously Presented) The method of claim 19, further comprising the steps of:

transmitting a deactivation message from the user to the redirector host system; and
upon receiving the deactivation message, prohibiting the redirection of data items for the user sending the deactivation message.

155. (Previously Presented) The method of claim 19, wherein the determining step includes the steps of:

accessing a user profile database including a list of authorized users; and
checking whether the user associated with the new data item is an authorized user to determine whether the new data item should be redirected to the user's mobile device.

156. (Previously Presented) The method of claim 19, wherein the determining step includes the steps of:

accessing a filter rules database including a list of filters to be applied to data items for a particular user; and

applying the filters to the new data item to determine whether the new data item should be redirected to the user's mobile device.

157. (Previously Presented) The method of claim 19, wherein the packaging step includes the step of addressing the electronic envelope using the electronic address of the user's mobile device.

158. (Previously Presented) The method of claim 19, wherein the data items are E-mail messages, and wherein the messaging host system is an E-mail host system.

159. (Previously Presented) The method of claim 19, wherein the user's mobile device is a laptop computer.

160. (Previously Presented) The method of claim 19, wherein the user's mobile device is a two-way paging computer.

161. (Previously Presented) The method of claim 160, wherein the two-way paging computer includes a wireless network interface for communicating with the redirector host system via a wireless data network.

162. (Previously Presented) The method of claim 161, wherein the redirector host system is coupled to the wireless data network via a wireless gateway system.

163. (Previously Presented) The method of claim 162, wherein the electronic envelope is addressed using the wireless data network address of the two-way paging computer.

164. (Previously Presented) The method of claim 19, wherein the messaging host system is an Internet Service Provider.

165. (Previously Presented) The method of claim 164, wherein the data items are E-mail messages, and wherein the Internet Service Provider includes a mail server program.

166. (Previously Presented) The method of claim 165, wherein the Internet Service Provider further includes a forwarding database coupled to the mail server program for detecting whether a new data item received at the mail server should be forwarded to a redirector host system, and for determining the electronic address of that redirector host system.

167. (Previously Presented) The method of claim 19, wherein the messaging host system and the redirector host system are coupled via the Internet.

168. (Previously Presented) The method of claim 19, wherein the redirector host system includes a further messaging host system.

169. (Previously Presented) The method of claim 19, wherein the redirector host system is incorporated with the messaging host system.

170. (Previously Presented) The method of claim 143, wherein the access mechanism for remotely configuring and reconfiguring the filtering rules is a web-page interface.

171. (Previously Presented) The method of claim 14,4 wherein the access mechanism for remotely configuring and reconfiguring the user profile database is a web-page interface.

172. (Previously Presented) The method of claim 19, further comprising the steps of:

configuring a user profile database for use by the redirector host system in determining whether the new data item should be redirected to the user's mobile data device; and

storing, within the user profile database, the electronic address of the user's mobile device.

173. (Previously Presented) The method of claim 172, further comprising the step of:

storing, within the user profile database, information regarding the type and configuration of the user's mobile device.

174. (Previously Presented) The method of claim 19, wherein the packaging step further includes the steps of:

converting the encrypted new data item into a compressed format; and

placing the compressed new data item into an electronic envelope that is addressed using the electronic address of the user's mobile device.